12333 INFO SHARING WORKING THREAD

Last week, the government released the long-awaited procedures permitting the intelligence community to share raw 12333 collected information more widely. This will be a working thread on those procedures.

(1) The procedures bill themselves as procedures to govern the sharing of information under 2.3 of EO 12333, which basically permits the IC to share info so IC elements can see if they need the info.

(1) The procedures exclude NSA SIGINT activities, which I think has the effect of making sure those don't operate with these limits.

(2) The procedures also exclude activities undertaken under NSCID-5 and NSCID-6, which I think has the effect of excluding joint NSA-CIA activities that already take place.

(2) Note the reference to PPD-28 (which reappears) refers to PPD-28 "and implementing procedures and any successor documents." That suggests there may be a lot more about PPD-28 we're not seeing, and that this Administration anticipates it will be changed.

(2-3) This section lays out what it claims to be limits on any info sharing agreements, which is basically a requirement that any entity getting NSA data must adopt procedures akin to those NSA adopts.

(3) Even if NSA tells another element of intelligence that would interest them, the element must make a formal request to get it. I suspect this is done so NSA can pretend it is not affirmatively giving away entire swaths of data.

(4) There's an odd definition of "reasonableness," which is the standard NSA always says it uses to comply with the Fourth

Amendment. It includes these measures of impact on US persons:

> e. (U) The likelihood that sensitive U.S. person information (USPI) will be found in the information and, if known, the amount of such information;
>
> f. (U) The potential for substantial harm, embarrassment, inconvenience, or unfairness to U.S. persons if the USPI is improperly used or disclosed;

That is, the measure is not if information is improperly access, but if accessing it might cause the US person substantial embarrassment of inconvenience.

(4) After the long section on reasonableness, the procedures then say NSA doesn't actually have to check the data set to make sure its measures of impact are valid.

(5) Those receiving NSA data are prohibited from tampering in politics.

> Not engage in any intelligence activity authorized by these Procedures, including disseminations to the White House, for the purpose of affecting the political process in the United States.

(5) Sharing agreements are covered by memoranda of agreement that last 3 years. Given the discussion of whether or not this enables Trump, I think it worth noting that any data sharing can be expanded before Trump's first term ends. Conversely, that implies that any president can impose new restrictions during a term.

(5) There's a squabble resolution process that goes to Secretary of Defense, then DNI for military units, and DNI for non-military.

(5) The procedures provide 3 different options for data possession that can count as sharing (one that was laid out in the 5240.01 revision released last year): the data remains in NSA's

systems, it goes to the IC cloud, it goes to the receiving entity's systems. The roll-out of the IC cloud in recent years was a technical precondition for this expanded sharing.

(6) Before the procedures talk about what the entities have to *do* with audits (that does come later), it has this to say about protecting audit records.

> Auditing records. Protect auditing records against unauthorized access, modification, or deletion, and retain these records for a sufficient period of time to verify compliance with the requirements of these Procedures.

Did they need to include this because audit records have been altered in the past?

(6) I've written a lot about the times (especially at FBI) where elements choose not to mark the source for their data, which allows for a lot of negative outcomes (such as hiding evidence source from defendants). So this passage makes me really furious.

> Marking o(files. Use reasonable measures to identify and mark or tag raw SIGINT files reasonably believed or known to contain USPI. Marking and tagging will occur regardless of the format or location of the information, or the method of storing it. When appropriate and reasonably possible, files and documents containing USPI will also be marked individually. In the case of certain electronic databases, if it is not reasonably possible to mark individual files containing USPI, a banner may be used before access informing users that they may encounter USPI.

There should be an initial requirement that all shared data retains its NSA SIGAD information, marking it both as NSA data and tracking how it

was collected. But this only asks that recipients mark data if it includes USPI, and even there allows the requirement to slide.

(7) The section prohibiting the selection of domestic (that is, between entirely US persons) is worthwhile. Except they don't tell you until later that metadata analysis (which for the purposes of this document is limited to contact chaining) is exempt from this. So this means law enforcement can use entirely NSA-collected raw data to do network analysis of entirely American communications.

(7) There are actually 3 different kinds of searches included in these procedures, which should get people to reconsider how they refer to "upstream" searches: searches on the identity of a communicant, searches mentioning a communicant, and searches on content (which comes a few pages later). Also note, it all relies on a new definition of "foreign" communications to mean what "international" used to, meaning they can access communications of a US person via that US person identifier if it happens internationally.

(7) The procedures let IC elements use US person identifiers for "selection" (a term designed to avoid "search") if that person is already approved for content spying with a FISA order, but not for metadata spying. Note they list 703 among the authorities in question, though at least until recently, they never used 703.

(7) One of the key prongs (of three) under which an element can spy on an American w/AG approval is redacted. I'll come back to this.

(8) Some of the reasons why the IC can spy on Americans are redacted. Given the items that appear on page 12, at least one of these is almost certainly a counterintelligence focus. The other may be counternarcotics or transnational crime.

(9) After having laid out how you can spy on Americans via their identifiers, the procedures now lay out how they might be swept up via their

content. Remember that this may mean "content of headers," and likely includes selectors for things like encryption keys. The selection term based collection permits the selection of US person communications (possibly, given the redaction, even between two US based US persons) if there will be significant FI or CI value.

(9) Minor point but the procedures explicitly use the phrase "defeat," which is a concept often redacted.

(9) There are no explicit protections for Attorney Client communications here, just a "call NSD for guidelines" rule, which is alarming.

(9) I'll come back to F, which is basically SPCMA on steroids, and probably a significant part of these sharing goals anyway. Effectively, this institutes SPCMA analysis, across IC elements, without some of the protections that have long been in place.

(10) Note, there seems to be flux in what metadata can be included as metadata (though there are reasonable definitions for metadata later). Also, ZERO of the oversight involves DOD.

(10) Retention is 5 years, so consistent with Section 309, which it cites.

(10) Note the reference to "data related to" communications to, from, or about US persons.

(10) The IC can only keep domestic communications in case of threat of death or bodily harm (but remember they include bodily harm to corporate persons in that).

(11) This is confusing. Right after saying it has to destroy domestic comms, it says that it can keep them if there is significant CI or FI value, and or anomalies showing a vulnerability to US comm service. This is sort of consistent with upstream 702, but not quite.

(11) The procedures treat government employee comes differently based on who they're talking

to, which is a tribute to how much this is about counterintelligence.

(11) The immediate notice of destruction incorporates a lesson they learned during 702, when such notices took time and US person stuff remained in the system in NSA even if destroyed at FBI.

(12) Note US person info can be disseminated for a non-exclusive list, though the list is quite extensive in any case.

(12) Info can be disseminated if someone is the target of hostile intelligence activities of a foreign power. This might make it easier for DHS to disseminate warnings.

(13) The auditing function described does *not* include an explicit exception for techs, whereas it would at NSA.

(14) Note the distinction between queries and retrievals. Added to selection, and we've got another set of not entirely sensical terms that are new.

(14) Note that throughout, the oversight mechanisms avoid any body that is statutorily independent, including both PCLOB and the IGs. So it should not be taken as credible.

(15) The first paragraph of VIII makes it clear they're parallel constructing this. No notice to defendants basically makes this unconstitutional, but the ID doesn't care.

(16) Throughout, there are designees allowed that will make it a cinch to put some of these sharing relationships in a box where no one will find them.

(16) The departures from procedures section doesn't include any deadlines for how long until notifications have to go out. Again, another easily exploited loophole.

(17) They added language to Obama's standard "does not create any rights" language to include

"nor do they place any limitation on otherwise lawful investigative and litigative prerogatives of the United States." Which sounds like *even more* parallel construction.

(17) As we'll see, "contact chaining" is defined to mean two hops. But because it isn't tied to anything, and because the definition of foreign power includes 3 degrees of separate for most things (engages in, aids or abets, or conspires), it really amounts to about 5 degrees of separation from any baddie.

(18) The definitions of metadata here are interesting (and different from the SPCMA one). First, on telephony metadata, they don't comment about location. The Internet metadata description is more descriptive than any I've seen, including routers passed during delivery. But there's so much that's not addressed in the definition, because it pretends to be exclusively about email.

(19) The definition of contact chaining does not include, as USAF chaining does, connection chaining. This reinforces my belief that the latter primarily serves a complimentary function, that of IDing all associated identities known by a provider. The contact chaining definition only permits two hops, but there's no limitation on target, which permits at least 5 and really an infinite number of hops.

(19) If just one recipient in a threat is not a USP, it does not count as domestic. Also, circumstances where someone doesn't have a REOP, like Twitter, does not count as domestic either.

(19) There used to be two distinct definitions: International, which was one end US, and foreign, which is both-ends foreign. I'm not sure why they've changed it such that any end foreign counts as foreign, but that seems problematic.

(20) Public info includes that which is available on request, or by purchase, meaning this may includes a lot of brokered lists and

the like (including advertising information).

(20) Definition of “selection” includes “cable address,” which seems like it could be very broadly interpreted.

(21) The definition of “selection term” is very useful (basically a boolean selection term), and should have been made public before.

(22) The USPI definition is notable both for its inclusions and exclusions. “Unique biometric records” is included, which seems like could be very broadly interpreted (and makes clear they’re throwing all the biometrics they have into this pot of analysis. There’s no specific mention of online identities (“names” and “unique titles” may incorporate that, but should be stated publicly). There’s also no mention of cookies or other session identifiers (which is especially notable given the silence about location data).

(22) The overhead reconnaissance language means they can use drone footage against us, so long as they don’t target it at us. Though some DirtBox uses would be problematic.